Кібернетична безпека та бізнес-розвідка в системі діагностики економічної безпеки підприємства

Cybernetic Security and Business Intelligence in the System of Diagnostics of Economic Security of the Enterprise

Руслан Скриньковський [1], Гжегож Павловські [2], Павло Гарасим [3], Олег Коропецький [1]
Ruslan Skrynkovskyy, Grzegorz Pawlowski, Pavlo Harasym, Oleh Koropetskyi

[1] *Lviv University of Business and Law*
99 Kulparkivska Street, Lviv, 79021, Ukraine

[2] *Zaklad Handlowo-Uslugowy BHP*
17 Kostrzynska Street, Gorzyca, 69-113, Poland

[3] *General Directorate of the National Police in the Lviv region*
3 General Hryhorenko Square, Lviv, 79007, Ukraine

DOI: 10.22178/pos.27-6

JEL Classification:
D83, L20, L86, M10

Received 20.09.2017
Accepted 25.10.2017
Published online
31.10.2017

Corresponding Author:
Ruslan Skrynkovskyy
uan_lviv@ukr.net

Анотація. Метою статті є визначення місця, ролі і особливостей кібернетичної безпеки та удосконалення схеми бізнес-розвідки в системі діагностики економічної безпеки підприємства. З'ясовано, що: 1) під кібернетичною безпекою підприємства слід розуміти стан захищеності кібернетичного простору підприємства в цілому або окремих об'єктів його інформаційної інфраструктури (комп'ютерної системи, комп'ютерних даних тощо) від ризику стороннього (зовнішнього) кібернетичного впливу, за якого забезпечується їх сталий розвиток і формування перспективи, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз інтересам підприємства; 2) основними складовими кібернетичної безпеки в системі діагностики економічної безпеки підприємства є: розвідка інформаційно-телекомунікаційних систем та криптосистем протиборчих сторін; кібернетичні впливи; захист власної інформаційної сфери. Встановлено, що головним завданням бізнес-розвідки в системі діагностики економічної безпеки підприємства є перевірка достовірності бізнес-інформації, забезпечення кібернетичного захисту інформаційного ресурсу, інформаційно-комунікаційних технологій та систем і виключення можливості дезінформації вищого керівництва підприємства з боку менеджерів (керівників) середньої ланки, постачальників, маркетингових посередників, клієнтури, конкурентів або контактних аудиторій підприємства. Перспективою подальших досліджень у даному напрямі є розроблення системи цілей полікритеріальної діагностики діяльності (економічної діагностики) підприємства (на засадах виокремлення та систематизації його діагностичних цілей) з урахуванням поданих результатів дослідження.

Ключові слова: підприємство; кібербезпека; бізнес-розвідка; інформація; комп'ютерні системи; економічна безпека; діагностика.

Abstract. The purpose of the article is to determine the place, the role and features of cybernetic security and improve the business intelligence scheme in the system of diagnosing economic security of the enterprise. It had been found out that: 1) the term "cybernetic security of an enterprise" should be understood as the state of the protection of the cybernetic space of the whole enterprise or individual objects of its information infrastructure (computer system, computer data, etc.) from the risk of external cybernetic influence, which ensures their sustainable development and the formation of prospects, as well as timely detection, prevention and neutralization of real and potential cybernetic interruptions and threats to the interests of the enterprise; 2) the main components of cybernetic security in the system of diagnostics of economic security of the enterprise are: investigation of information and telecommunication systems and cryptosystems of the opposing sides; cybernetic effects; protection of information sphere. It was established that

the main task of business intelligence in the system of diagnosing economic security of the enterprise is the verification of the reliability of business information, the provision of cybernetic protection of information resources, information and communication technologies and systems and the elimination of the possibility of misinformation of senior management by the managers of the middle level, suppliers, marketing intermediaries, clientele, competitors or contact audiences of the enterprise. The prospect of further research in this direction is the development of a system of goals of the polycriterial diagnostics of the activity (economic diagnostics) of the enterprise (on the basis of the isolation and systematization of its diagnostic purposes), taking into account the presented results of the study.

Keywords: enterprise; cyber security; business intelligence; information; computer systems; economic security; diagnostics.

ВСТУП

Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладної розробки та реалізації конкретних заходів із кібербезпеки і кіберзахисту підприємств (установ, організацій) відповідно до ключових пріоритетів та напрямів реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Аналіз останніх досліджень і публікацій свідчить про те, що вагомий науково-практичний внесок у вирішення окремих проблемних питань (аспектів) у сфері кібербезпеки та кіберзахисту підприємств (установ, організацій) зробили такі науковці, як В. Бурячок [1], В. Братюк [2], О. Волох [3], Є. Воронюк [4], С. Гахов [5], С. Кавун [6], В. Ляшевський [7], Д. Маріц [8], Ю. Мороз, Ю. Цаль-Цалко [9], Е. Хемфрі [10] та інші. Водночас, віддаючи належне високому рівню наукових доробок перелічених вище авторів, зазначимо, що сьогодні не до кінця вивченими залишаються питання щодо кібернетичної безпеки та бізнес-розвідки в системі діагностики економічної безпеки підприємства у структурі системи цілей економічної діагностики підприємства, зокрема дискусійними є: 1) визначення місця, ролі і особливостей кібернетичної безпеки в системі діагностики економічної безпеки підприємства; 2) погляди (бачення) на формування (розроблення) схеми бізнес-розвідки в системі діагностики економічної безпеки підприємства. Все це обумовлює актуальність та доцільність дослідження у цьому напрямі.

Тому *метою статті* є визначення місця, ролі і особливостей кібернетичної безпеки та удосконалення схеми бізнес-розвідки в системі діагностики економічної безпеки підприємства.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результати вивчення й аналізу наукових, методичних та прикладних матеріалів за проблематикою діагностики, зокрема [11, 12, 13, 14, 15, 16, 17] та іншої наукової літератури, приведеної у [18], дають можливість стверджувати, що діагностика діяльності (економічна діагностика) підприємства (установи, організації) – це процес ідентифікації, аналізу й оцінювання стану підприємства і тенденцій його зміни (тобто зміни стану) на основі відповідних бізнес-індикаторів з метою розроблення рекомендацій щодо усунення проблемних моментів (загроз) і слабких сторін суб'єкта господарювання та/або використання шансів (можливостей) умов діяльності підприємства для забезпечення якісно нового рівня його ефективності, розвитку і формування перспективи з урахуванням: 1) впливу взаємозалежних факторів впливу зовнішнього середовища (непрямої та прямої дії) і внутрішніх змінних (факторів внутрішнього середовища) підприємства (працівники, цілі і завдання, інформація, структура, технологія та ресурси); 2) юридичної та соціальної відповідальності підприємства у сфері економіки й управління підприємствами. Водночас з'ясовано, що структура системи цілей діагностики діяльності підприємства (установи, організації), виходячи із виокремлення та систематизації діагностичних цілей (елементних, часткових, комплексних) системи цілей економічної діагностики підприємства, містить таку структурну складову групи часткових діагностичних цілей (або часткову діаг-

ностичну ціль), як діагностика економічної безпеки підприємства [18].

В свою чергу науковці [4] прийшли до висновку, що діагностика та аналіз економічної безпеки підприємства (установи, організації) полягає у моніторингу її складових, а саме: 1) фінансової; 2) інтелектуальної; 3) кадрової; 4) технологічної; 5) правової; 6) силової; 7) ринкової; 8) екологічної; 9) інформаційної; 10) інтерфейсної.

З огляду на це і виходячи з результатів виконаних досліджень [19], встановлено, що ключовими бізнес-індикаторами системи діагностики економічної безпеки підприємства (як часткової діагностичної цілі системи цілей економічної діагностики підприємства [11, 18]) є такі: 1) рівень безпеки за фінансовою складовою; 2) рівень безпеки за кадрово-інтелектуальною складовою; 3) рівень безпеки за інноваційно-техніко-технологічною складовою; 4) рівень безпеки за інвестиційною складовою; 5) рівень безпеки за маркетингово-ринковою складовою; 6) рівень безпеки за політико-правовою складовою; 7) рівень безпеки за обліково-аналітико-інформаційною складовою; 8) рівень безпеки за екологічною складовою [19].

Поряд із тим варто наголосити, що сьогодні основою розвитку (як бізнес-процесів, так і результату) сучасного підприємства (установи, організації) є його інформаційна інфраструктура, яка створюється і підтримується власними силами підприємства і/або силами компанії-аутсорсера. З одного боку, застосування інформаційних технологій в управлінні підприємством (спільно з інформаційними ресурсами, технічними засобами, програмним забезпеченням та інтелектуальними технологічними процесами) створює умови для прийняття обгрунтованих управлінських рішень (поточних, перспективних) та якісно змінює бізнес-процеси (внутрішні, зовнішні), спрямованих на підвищення загального рівня ефективності та результативності діяльності підприємства. З іншого боку, існування певних бізнес-процесів підприємства в кібернетичному просторі створює умови та можливості стороннього кібернетичного впливу на них з метою комп'ютерного шахрайства (на основі несанкціонованого створення, зберігання, обміну, обробки чи знищення комп'ютерних даних тощо) або з іншою недобросовісною метою [5, 20, 21, 22, 23]. Звідси очевидно, що кібернетична безпека є структурною складовою діагностики економічної безпеки у структурі системи цілей економічної діагностики підприємства.

Тут доцільно також звернути особливу увагу на результати досліджень [24], згідно яких видно, що у науковій літературі сутність (зміст) поняття «економічна безпека підприємства» розглядається у різних аспектах, зокрема як:

1) стан господарюючого суб'єкта, що характеризується високим ступенем захищеності від існуючих небезпек та загроз;

2) стан найбільш ефективного використання корпоративних ресурсів для стабільного функціонування підприємства;

3) захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, що забезпечується системою заходів спеціального, фінансово-економічного, організаційного та соціального характеру;

4) стан виробничих відносин і організаційних зв'язків, при яких забезпечується стабільність функціонування та прогресивний розвиток підприємства;

5) забезпечення умов збереження майна та комерційної таємниці [24].

В контексті цього (за результатами дослідження) з'ясовано, що:

1) кібернетична безпека підприємства – це стан захищеності кібернетичного простору підприємства в цілому або окремих об'єктів його інформаційної інфраструктури (комп'ютерної системи, комп'ютерних даних тощо) від ризику стороннього (зовнішнього) кібернетичного впливу, за якого забезпечується їх сталий розвиток і формування перспективи, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз інтересам підприємства [1, 23];

2) основними складовими кібернетичної безпеки в системі діагностики економічної безпеки підприємства є:

- розвідка інформаційно-телекомунікаційних систем та криптосистем протиборчих сторін;

- кібернетичні впливи;

- захист власної інформаційної сфери [1];

3) характерними видами кібернетичних ризиків (або ризиків стороннього кібернетичного впливу) та напрямів кіберстрахування є:

- ризики втрати інформації (комп'ютерних даних) та порушення роботи систем при зламі паролів доступу або внаслідок DDoS-атаки;

- ризики фінансових втрат через порушення роботи (функціонування) комп'ютерних систем та на відновлення програмного забезпечення і/або інформації (комп'ютерних даних) внаслідок дій кіберзлочинців;

- ризики фінансових втрат власників даних за регрес-позовами при викраденні, зберіганні, використанні, знищенні або поширенні (розголошенні) кіберзлочинцями персональної інформації;

- ризики фінансових втрат за кібервимаганням (здирництвом) при вірусному блокуванні комп'ютерних систем або баз даних [2];

4) загрози кібернетичній безпеці підприємства (установи, організації) актуалізуються через дію таких чинників:

- невідповідність інфраструктури електронних комунікацій підприємства, рівня її розвитку та захищеності сучасним вимогам;

- недостатня ефективність суб'єктів сектору економічної безпеки та бізнес-розвідки підприємства у протидії кіберзагрозам спеціального, фінансово-економічного, організаційного та соціального характеру;

- низький загальний рівень обізнаності працівників підприємства в питаннях інформаційної та кібернетичної безпеки;

- недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібернетичної безпеки підприємства інформаційної інфраструктури і електронних інформаційних ресурсів;

- безсистемність заходів кібернетичного захисту інформаційного ресурсу, інформаційно-комунікаційних технологій та систем підприємства тощо [3, 5, 6, 7, 8, 23, 25].

Крім цього, на основі аналізу інформації у [10, 26] встановлено, що:

1) кібернетичні ризики існують завжди, адже підприємства (установи, організації) використовують однакові технології та програми, спілкуються через мережу Internet тощо;

2) багато програм, розроблюваних для захисту організацій від кіберзагроз, розробляють з посиланням на стандарти ISO/IEC 27001 та ISO/IEC 27002:2005 «Інформаційні технології. Методи убезпечення. Кодекс практики з управління інформаційною безпекою» [10];

3) згідно ст. ст. 2–5 Конвенції про кіберзлочинність [26] основними правопорушеннями проти конфіденційності, цілісності та доступності комп'ютерних даних і систем є:

- незаконний доступ;

- нелегальне перехоплення;

- втручання у дані;

- втручання у систему;

- зловживання пристроями.

Поряд з тим, у науковій праці [7] зазначено, що ключовими пріоритетами (цілями), які визначені для систем управління інформаційною безпекою сучасного бізнес-процесу (з урахуванням захисту від кіберзагроз), є:

- стабільність бізнесу (А);

- захист бізнес-інтересів власників (В);

- підвищення рівня довіри бізнес-партнерів та клієнтів (С).

З огляду на викладене вище Л. Дегтярьова та В. Ляшевський [7] стверджують, що для того, щоб подані цілі (А, В, С) були досягнуті, необхідно вирішити такі завдання:

1) обмежити доступ до бази даних (спеціальної інформації [27]), визначеної як службова таємниця;

2) визначити та здійснити адміністративні заходи для виявлення загроз безпеці інформаційних ресурсів;

3) з'ясувати можливі мотиви, що мають на меті нанесення збитків (фінансових, матеріальних, моральних);

4) забезпечити ефективне й результативне використання правових, організаційних і технічних засобів забезпечення інформаційної безпеки;

5) створити умови для виявлення кібернетичних ризиків тощо [7].

Беручи до уваги зазначене, тут доцільно відмітити, що одним із інструментів сучасного менеджменту (в умовах конкурентної боротьби) є застосування прогресивних методів бізнес-розвідки в забезпеченні діяльності служб економічної безпеки, головним завданням якої є перевірка достовірності бізнес-інформації, забезпечення кібернетичного

захисту інформаційного ресурсу, інформаційно-комунікаційних технологій та систем і виключення можливості дезінформації вищого керівництва підприємства з боку менеджерів (керівників) середньої ланки, постачальників, маркетингових посередників, клієнтури, конкурентів або контактних аудиторій підприємства [28].

Блок-схема процесу бізнес-розвідки в системі діагностики економічної безпеки підприємства (установи, організації) представлена на рис. 1.

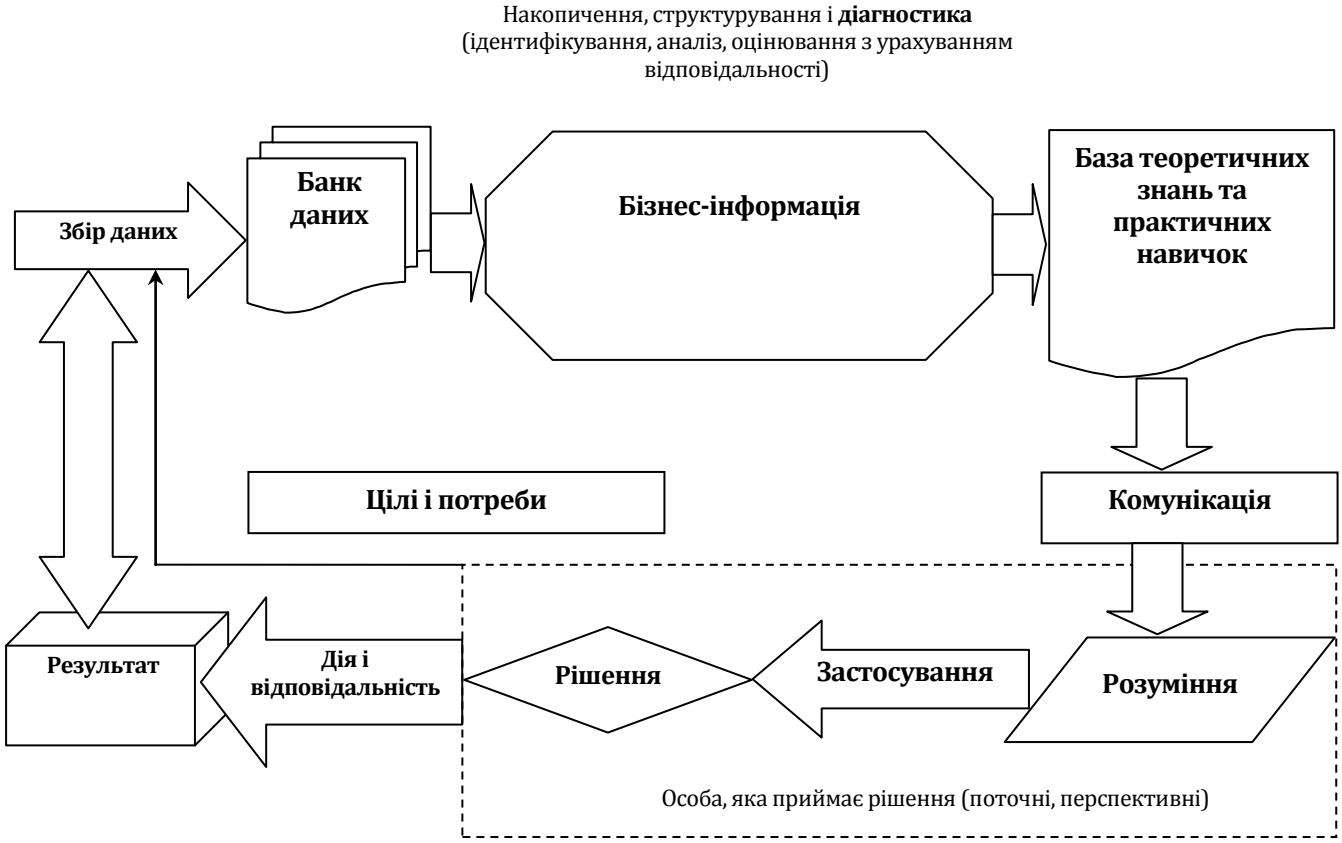

Рисунок 1 – Блок-схема бізнес-розвідки в системі діагностики економічної безпеки підприємства (установи, організації), удосконалено на основі [28]

Для довідки: 07.06.2017 р. Національне агентство із забезпечення якості вищої освіти (НАЗЯВО) [29] погодило освітній стандарт спеціальності «Кібербезпека» для бакалаврського рівня. «Нині, в умовах російської агресії, ми досить гостро відчуваємо потребу в фахівцях з кібербезпеки. Затвердження нового стандарту дозволить нам готувати спеціалістів високого рівня, готових застосовувати здобуті знання у реальних умовах та реагувати на виклики часу … .», – зазначив перший заступник Міністра освіти і науки України В. Ковтунець [30].

ВИСНОВКИ

Результати дослідження доводять, що під кібернетичною безпекою підприємства слід розуміти стан захищеності кібернетичного простору підприємства в цілому або окремих об'єктів його інформаційної інфраструктури (комп'ютерної системи, комп'ютерних даних тощо) від ризику стороннього (зовнішнього) кібернетичного впливу, за якого забезпечується їх сталий розвиток і формування перспективи, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз інтересам підприємства. З'ясовано, що основними складовими кібернетичної безпеки в системі діагностики економічної безпеки підприємства є: розвідка інформаційно-телекомунікаційних систем та криптосистем протиборчих сторін; кібернетичні впливи; захист власної інформаційної сфери. Встановлено, що головним завданням бізнес-розвідки в системі діагностики економічної безпеки підприємства є перевірка достовір-

ності бізнес-інформації, забезпечення кібернетичного захисту інформаційного ресурсу, інформаційно-комунікаційних технологій та систем і виключення можливості дезінформації вищого керівництва підприємства з боку менеджерів (керівників) середньої ланки, постачальників, маркетингових посередників, клієнтури, конкурентів або контактних аудиторій підприємства.

Перспективою подальших досліджень у даному напрямі є розроблення системи цілей полікритеріальної діагностики діяльності (економічної діагностики) підприємства (на засадах виокремлення та систематизації його діагностичних цілей) з урахуванням поданих результатів дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Buriachok, V. L., & Bohush, V. M. (2014). Rekomendatsii shchodo rozrobky ta zaprovadzhennia profiliu navchannia «Kibernetychna bezpeka» v Ukraini [Guidelines for the development and implementation training profile «cyber security» in Ukraine]. *Ukrainian Scientific Journal of Information Security, 20*(2), 126–131. doi: 10.18372/2225-5036.20.7297 (in Ukrainian)
[Бурячок, В. Л., & Богуш, В. М. (2014). Рекомендації щодо розробки та запровадження профілю навчання «Кібернетична безпека» в Україні. *Безпека інформації, 20*(2), 126–131. doi: 10.18372/2225-5036.20.7297].

2. Bratiuk, V. P. (2015). Sutnist kiber-zlochyniv ta strakhovyi zakhyst vid kiber-ryzykiv v Ukraini [Essence of cyber crimes and insurance protection from cyber risks in Ukraine]. *Actual Problems of Economics, 9*, 421–427].
[Братюк, В. П. (2015). Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки, 9*, 421–427].

3. Volokh, O. K. (2016). Pytannia kibernetychnoi bezpeky v umovakh rozbudovy informatsiinoho suspilstva [Question of cyber security under development information society]. *Yurydychnyi naukovyi elektronnyi zhurnal, 4*, 104–107 (in Ukrainian)
[Волох, О. К. (2016). Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. *Юридичний науковий електронний журнал, 4*, 104–107].

4. Ivashchenko H. A., & Voroniuk, Ie. V. (2017). Kibernetychna bezpeka v systemi diahnostyky ta analizu ekonomichnoi bezpeky pidpryiemstva [Cyber security in the diagnosis and analysis economic security]. *Young Scientist, 1*, 605–608 (in Ukrainian)
[Іващенко Г. А., Воронюк, Є. В. (2017). Кібернетична безпека в системі діагностики та аналізу економічної безпеки підприємства. *Молодий вчений, 1*, 605–608].

5. Hakhov, S. O. (2016). Zastosuvannia metodiv pravovoho rehuliuvannia pid chas zdiisnennia orhanizatsiinykh zakhodiv shchodo kibernetychnoho zakhystu informatsiinykh system pidpryiemstv, ustanov ta orhanizatsii [Application of methods of legal regulation during the implementation of organizational measures for cybernetic protection of information systems of enterprises, institutions and organizations]. *Suchasnyi zakhyst informatsii, 3*, 67–71 (in Ukrainian)
[Гахов, С. О. (2016). Застосування методів правового регулювання під час здійснення організаційних заходів щодо кібернетичного захисту інформаційних систем підприємств, установ та організацій. Сучасний *захист інформації, 3*, 67–71].

6. Kavun, S. V., & Holubiev, V. O. (2013). Analiz kiberzlochynnosti u sferi ekonomichnoi bezpeky [Analysis of cybercrime in the field of economic security]. *Naukovi pratsi Chornomorskoho derzhavnoho universytetu imeni Petra Mohyly. Seriia: Komp'iuterni tekhnolohii, 229*(217), 9–13 (in Ukrainian)
[Кавун, С. В., & Голубєв, В. О. (2013). Аналіз кіберзлочинності у сфері економічної безпеки. *Наукові праці Чорноморського державного університету імені Петра Могили. Серія: Комп'ютерні технології, 229*(217), 9–13].

7. Dehtiarova, L. M., & Liashevskyi, V. H. (2017). Praktychni pryiomy ta kerivni pryntsypy rozrobky kompleksiv informatsiinoi bezpeky [Practical techniques and management principles development of systems of information security]. *Systemy upravlinnia, navihatsii ta zv'iazku, 2*(42), 94–97 (in Ukrainian)
[Дегтярьова, Л. М., & Ляшевський, В. Г. (2017). Практичні прийоми та керівні принципи розробки комплексів інформаційної безпеки. *Системи управління, навігації та зв'язку, 2*(42), 94–97].

8. Marits, D. O. (2015). "Kiberataka" – viina maibutnoho ["Kiberataka" - the war of the future]. *Informatsiia i pravo, 3*(15), 104–109 (in Ukrainian)
[Маріц, Д. О. (2015). «Кібератака» – війна майбутнього. *Інформація і право, 3*(15), 104–109].

9. Moroz, Ju. Ju., & Cal'-Calko, Ju. S. (2017). Oblikova politika pidpriємstva ta її kiberbezpeka [The accounting policies of the enterprise and its cyber security]. *Oblik, analiz i kontrol' v umovah suchasnih koncepcij upravlinnja ekonomichnim potencialom i rinkovoju vartistju pidpriємstva, 4*(1), 8–11 (in Ukrainian)
[Мороз, Ю. Ю., & Цаль-Цалко, Ю. С. (2017). Облікова політика підприємства та її кібербезпека. Облік, аналіз і контроль в умовах сучасних концепцій управління економічним потенціалом і ринковою вартістю підприємства, 4(1), 8–11].

10. Khemfri, E. (2013). Diialnist z kiber-bezpeky. Rishennia dlia biznesu [Cybersecurity activities. Solutions for business]. *Standartyzatsiia. Sertyfikatsiia. Yakist, 1*, 16–18 (in Ukrainian)
[Хемфрі, Е. (2013). Діяльність з кібер-безпеки. Рішення для бізнесу. *Стандартизація. Сертифікація. Якість, 1*, 16–18].

11. Melnyk, O. H. (2010). *Systemy diahnostyky diialnosti mashynobudivnykh pidpryiemstv: polikryterialna kontseptsiia ta instrumentarii* [Systems of diagnostics of activity of machine-building enterprises: polycrystalline concept and tools]. Lviv: Vydavnytstvo Lvivskoi politekhniky (in Ukrainian)
[Мельник, О. Г. (2010). *Системи діагностики діяльності машинобудівних підприємств: полікритеріальна концепція та інструментарій*. Львів: Видавництво Львівської політехніки].

12. Bol'shakov, V. V. (1989). *Problemnaja diagnostika razvitija organizacij i predprijatij* [Problem diagnosis of the development of organizations and enterprises]. Vil'njus: Lit-NIITI (in Russian)
[Большаков, В. В. (1989). *Проблемная диагностика развития организаций и предприятий*. Вильнюс: Лит-НИИТИ].

13. Vasilenko, V. A. (2006). *Diagnostika ustojchivogo razvitija predprijatij* [Diagnostics of sustainable development of enterprises]. Kiev: Centr uchebnoj literatury (in Russian)
[Василенко, В. А. (2006). *Диагностика устойчивого развития предприятий*. Киев: Центр учебной литературы].

14. Voronkova, A. Je. (2000). *Strategicheskoe upravlenie konkurentosposobnym potencialom predprijatija: diagnostika i organizacija* [Strategic management of the competitive potential of the enterprise: diagnostics and organization]. Lugansk: Izd-vo VNU (in Russian)
[Воронкова, А. Э. (2000). *Стратегическое управление конкурентоспособным потенциалом предприятия: диагностика и организация*. Луганск: Изд-во ВНУ].

15. Hrechan, A. P., & Radionova, N. Y. (2011). Diahnostyka efektyvnosti diialnosti pidpryiemstv [Diagnostics of efficiency of activity of enterprises]. *Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 10*, 56–61 (in Ukrainian)
[Гречан, А. П., & Радіонова, Н. Й. (2011). Діагностика ефективності діяльності підприємств. *Вісник Східноукраїнського національного університету імені Володимира Даля, 10*, 56–61].

16. Glazov, M. M. (1998). *Jekonomicheskaja diagnostika predprijatij: novye reshenija* [Economic diagnostics of enterprises: new solutions]. Saint-Petersburg: SPbGUJeF (in Russian)
[Глазов, М. М. (1998). *Экономическая диагностика предприятий: новые решения*. Санкт-Петербург: СПбГУЭФ].

17. Kryvoviaziuk, I. V. (2012). *Funktsionuvannia ta rozvytok pidpryiemstv v umovakh kryzy: systemno-analitychnyi pidkhid* [Functioning and development of enterprises in a crisis: a system-analytical approach]. Lutsk: LNTU (in Ukrainian)
[Кривов'язюк, І. В. (2012). *Функціонування та розвиток підприємств в умовах кризи: системно-аналітичний підхід*. Луцьк: ЛНТУ].

18. Pawlowski, G. (2017). *Rozvytok systemy upravlinskoi diahnostyky pidpryiemstva* [Development of the system of management diagnostics of the enterprise] (Doctoral dissertation). Retrieved from http://irbis-nbuv.gov.ua/ASUA/1257760 (in Ukrainian)
[Павловські, Г. (2017). *Розвиток системи управлінської діагностики підприємства* (Кандидатська дисертація). URL: http://irbis-nbuv.gov.ua/ASUA/1257760].

19. Skrynkovskyy, R. (2015). Ekonomichna bezpeka pidpryiemstva: sutnist, klasyfikatsiia ta systema diahnostyky [Economic security of enterprise: nature, classification and system of diagnostics]. *Hlobalni ta natsionalni problemy ekonomiky, 3*, 414–418 (in Ukrainian)
[Скриньковський, Р. М. (2015). Економічна безпека підприємства: сутність, класифікація та система діагностики. *Глобальні та національні проблеми економіки, 3*, 414–418].

20. Noga, I., Skrynkovskyy, R., & Pawlowski, G. (2016). Diahnostyka efektyvnosti zastosuvannia informatsiinykh tekhnolohii v upravlinni pidpryiemstvamy [The Diagnostics of Efficiency of Applying Information Technology in the Management of Enterprises]. *Business Inform, 9*, 241–245 (in Ukrainian)
[Нога, І. М., Скриньковський, Р. М., & Павловські, Г. (2016). Діагностика ефективності застосування інформаційних технологій в управлінні підприємствами. *Бізнес Інформ, 9*, 241–245].

21. Skrynkovskyy, R., Pawlowski, G., & Vorobiov, V. (2016). Diahnostyka efektyvnosti kontrolinhu biznes-protsesiv pidpryiemstva [The Diagnostics of Efficiency of Controlling Business Processes]. *Business Inform, 8*, 154–159 (in Ukrainian)
[Скриньковський, Р. М., Павловські, Г., & Воробйов, В. В. (2016). Діагностика ефективності контролінгу бізнес-процесів підприємства. *Бізнес Інформ, 8*, 154–159].

22. Belskyi, Yu. (2014). Shchodo vyznachennia poniattia kiberzlochynu [Concerning the definition of cybercrime]. *Yurydychnyi visnyk,6*, 414–418 (in Ukrainian)
[Бельський, Ю. (2014). Щодо визначення поняття кіберзлочину. *Юридичний вісник,6*, 414–418].

23. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt [Information and cybersecurity: sociotechnical aspect]. Kyiv: DUT (in Ukrainian)
[Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., & Толюпа, С. В. (2015). Інформаційна та кібербезпека: соціотехнічний аспект. Київ: ДУТ].

24. Hnylytska, L. (2013). Osnovy ekonomichnoi bezpeky pidpryiemstva [Fundamentals of economic security of the enterprise]. *Bukhhalterskyi oblik i audyt, 7*, 41–48 (in Ukrainian)
[Гнилицька, Л. (2013). Основи економічної безпеки підприємства. *Бухгалтерський облік і аудит, 7*, 41–48].

25. Stratehiia kiberbezpeky Ukrainy [Cybersecurity Strategy of Ukraine] (Ukraine), 15 March 2016, No 96/2016. Retrieved September 1, 2017, from http://zakon2.rada.gov.ua/laws/show/96/2016 (in Ukrainian)
[Стратегія кібербезпеки України (Україна), 15 березня 2016, № 96/2016. Актуально на 01.09.2017. URL: http://zakon2.rada.gov.ua/laws/show/96/2016].

26. Konventsiia pro kiberzlochynnist [Cybercrime Convention] (Council of Europe), 23 November 2001. Retrieved September 1, 2017, from http://zakon2.rada.gov.ua/laws/show/994_575 (in Ukrainian)
[Конвенція про кіберзлочинність (Рада Європи), 23 листопада 2001. Актуально на 01.09.2017. URL: http://zakon2.rada.gov.ua/laws/show/994_575].

27. Skrynkovskyi, R. M., Kramar, R. I., & Harasym, P. S. (2016). Diahnostyka efektyvnosti systemy zakhystu informatsii na pidpryiemstvi ta vidpovidalnist za porushennia zakonodavstva pro komertsiinu taiemnytsiu [Diagnostics of information security efficiency at enterprise and responsible for violation of commercial secrecy legislation]. *Porivnialno-analitychne pravo, 1*, 225–228 (in Ukrainian)
[Скриньковський, Р. М., Крамар, Р. І., & Гарасим, П. С. (2016). Діагностика ефективності системи захисту інформації на підприємстві та відповідальність за порушення законодавства про комерційну таємницю. *Порівняльно-аналітичне право, 1*, 225–228].

28. Hetman, O. O., & Shapoval, V. M. (2007). *Ekonomichna diahnostyka* [Economic diagnostics]. Kyiv: Tsentr navchalnoi literatury (in Ukrainian)
[Гетьман, О. О., & Шаповал, В. М. (2007). *Економічна діагностика*. Київ: Центр навчальної літератури].

29. Natsionalne ahentstvo iz zabezpechennia yakosti vyshchoi osvity. (2017). Istoriia ahentstva [History]. Retrieved September 1, 2017, from http://naqa.gov.ua/istoriia-ahentstva (in Ukrainian)
[Національне агентство із забезпечення якості вищої освіти. (2017). Історія агентства. Актуально на 01.09.2017. URL: http://naqa.gov.ua/istoriia-ahentstva].

30. Ministerstvo osvity i nauky Ukrainy. (2017). NAZIaVO pochynaie robotu: pohodzheno pershyi standart vyshchoi osvity. Retrieved June 7, 2017, from http://mon.gov.ua/usi-novivni/novini/2017/06/07/nazyavo-pochinae-robotu-pogodzheno-pershij-standart-vishhoyi-osviti (in Ukrainian)
[Міністерство освіти і науки України. (2017). НАЗЯВО починає роботу: погоджено перший стандарт вищої освіти. Актуально на 07.06.2017. URL: http://mon.gov.ua/usi-novivni/novini/2017/06/07/nazyavo-pochinae-robotu-pogodzheno-pershij-standart-vishhoyi-osviti].